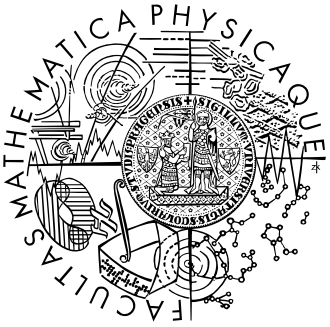
Univerzita Karlova v Praze

Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Samuel Čarnoký

Algoritmus pro kvantovou faktorizaci

Katedra algebry

Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.

Studijní program: Matematika

2008

Ďakujem môjmu vedúcemu za usmernenie, trpezlivosť a za odpovede na moje početné otázky.

Prehlasujem, že som svoju bakalársku prácu vypracoval samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce a jej zverejňovaním.

V Prahe dňa 6. 8. 2008 Samuel Čarnoký

Obsah

Názov práce: Algoritmus pre kvantovou faktorizaci

Autor: Samuel Čarnoký

Katedra: Katedra Algebry

Vedúci bakalárskej práce: Mgr. Libor Barto, Ph.D.

e-mail vedúceho : libor.barto@gmail.com

Abstrakt: V predloženej práci predstavujeme princípy fungovania kvantových počítačov, využívajúcich kvantové javy na urýchlenie riešenia niektorých úloh. Popisujeme kvantové algoritmy, ktoré prinášajú exponenciálne zrýchlenie oproti klasickému prístupu. Dôraz kladieme na Shorov faktorizačný algoritmus, rozkladajúci čísla v polynomiálnom čase a možné dôsledky jeho implementácie v oblasti informačnej bezpečnosti. Venujeme sa partiám z teórie čísel, ktoré využíva a predstavujeme kryptosystém RSA. Prevádzame problém faktorizácie na problém nájdenia rádu prvku. V závere predstavujeme úskalia realizácie kvantových výpočtov v praxi, ale aj úspechy a vízie do budúcnosti.

Kľúčové slová : kvantový počítač, kvantová mechanika, faktorizácia

Title: Quantum Factoring Algorithm

Author: Samuel Čarnoký

Department: Department of Algebra

Supervisor: Mgr. Libor Barto, Ph.D.

Supervisor's email address : libor.barto@gmail.com

Abstract: In this work we present basic principles of quantum computers, devices using quantum phenomena to solve hard problems. We describe quantum algorithms that bring exponential improvement over classical approach. We describe Shor's factoring algorithm, working in polynomial time and it's consequences in the field of information security. RSA cipher and selected parties from number theory needed for this algorithm are introduced. It's shown, how the integer factorisation problem can be converted to the finding order problem. We mention obstacles in physical realisation of quantum computers, recent achievements and visions.

Keywords : quantum computer, quantum mechanics, factorisation

Kapitola 1

Kvantový model

1.1 Úvod

Rast výkonu počítačov celkom verne nasleduje Moorov zákon, ktorý hovorí, že sa každých 18 mesiacov počet tranzistorov na lacno vyrobiteľných čipoch zdvojnásobí. Tento úžasný exponenciálny nárast však znamená, že inžinieri nevyhnutne narazia na hranicu, pod ktorú už nebude možné zmenšovať výrobné technológie. Na atomárnej úrovni už nebude možné skonštruovať potrebné komponenty. Avšak tam, kde éra klasických počítačov teoreticky končí, sa najsilnejšie prejavujú kvantové javy. Ich pochopenie a využitie umožnuje posunúť výpočetný výkon nad možnosti klasických počítačov.

Myšlienka použiť zákony kvantovej mechaniky na výpočty sa začala objavovať v osemdesiatych rokoch . Bolo síce dokázané, že je možné simulovať kvantový výpočet na klasickom počítači, čo znamená že kvantový prístup neprináša nič fundamentálne nové, avšak simulácia musí byť exponeniálne náročná [4]. Tento fakt je základným dôvodom pre obrovský potenciál kvantových počítačov. Príkladom je kvantový algoritmus rozkladajúci čísla na súčin prvočísel v polynomiálnom čase, ktorý popíšeme.

1.2 Princípy kvantovej mechaniky

V tejto časti predstavíme základné princípy kvantovej teórie, s dôrazom na tie, ktoré sú najrelevantnejšie pre oblasť kvantových výpočtov. Ako každá fyzikálna teória, aj kvantová mechanika predstavuje postuláty, ktoré slúžia ako základ a zväzujú jej abstraktný matematický model s realitou sveta, ktorý sa snaží popísať.

Postulát 1

Ku každému uzavretému kvantovému systém je asociovaný komplexný Hilbertov priestor H. Stavu systému odpovedá hodnota vektoru s normou 1 v tomoto priestore [2].

Najjednoduchší kvantový systém je reprezentovaný dvojrozmerným komplexným vektorovým priestorom $\mathbb{C}^2$. Stavy v ňom sú vyjadrené dvojicami komplexných čísel α a β , takými že $|\alpha|^2+|\beta|^2=1$. Pri vyjadrení bázových vektorov tohto priestoru

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix} \quad \text{a} \quad |1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$$

dostávame obvyklé vyjadrenie základnej jednotky kvantovej informácie, ktorá opisuje stav $|\psi\rangle$ nášho jednoduchého systému ako

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle.$$

Tento stav sa nazýva qubit, čo je skrátený názov pre quantum bit.

Prípad l qubitového systému, takzvaného kvantového registra, sa modeluje tenzorovým súčinom l jednoqubitových systémov $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$. Fázou budeme v ďalšom rozumieť uhol v exponenciálnej notácii komlexného čísla pri bázovom stave, amplitúdou zas absolútnu hodnotu tohto komplexného čísla. Na troch klasických bitoch sa číslo 0 reprezentuje ako 000, číslo 7 ako 111 a číslo 5 ako 101. Skúsme pre ilustráciu reprezentovať čísla 0 až 7 qubitmi. Bežne sa volia v jednotlivých qubitoch také bázové stavy, aby výsledný symbolický zápis dával zápis vyjadrovaného čísla v dvojkovej sústave. Pre číslo 5 použijeme kvantový register v stave

$$|1\rangle \otimes |0\rangle \otimes |1\rangle = |101\rangle = |5\rangle \ .$$

Vidíme tri rôzne symbolické zápisy bázového stavu kvantového registra pozostávajúceho z troch qubitov, ktorý vyjadruje 5. Takto je možné pohodlne reprezentovať čísla 0 až 7 . Nie je ale dôvod, prečo by mal byť každý qubit v registri len v zákadnom bázovom stave. Uvážme situáciu, keď je prvý qubit v stave $1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ Potom podmienka $|\alpha|^2 + |\beta|^2 = 1$ je splnená,

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}|001\rangle + \frac{1}{\sqrt{2}}|101\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |5\rangle)$$

a to znamená, že kvantový register uchováva v sebe hodnoty 1 a 5 súčasne. Hovoríme o kvantovej superpozícii. Nie je tažké si predstaviť superpozíciu, pri ktorej sme schopní uchovať všetkých 2^n hodnôt, kde n je počet qubitov tvoriacich register. Pred tým, ako tento fakt využijeme pri výpočtoch, zaoberajme sa chvíľu otázkou, ako sa kvantový stav vyvýja v čase.

Postulát 2

Vývoj uzavretého kvantového systém je daný unitárnym operátorom U, ktorý stav $|\psi\rangle$ v čase t_1 pretransformuje do stavu v čase t_2 tak, že $|\psi'\rangle = U|\psi\rangle$ [2].

Unitárne operátory zachovávaju normu, preto vznikne platný kvantový stav. Použijeme ich na vybudovanie matematického modelu kvantového počítača. Nestačí však vedieť iba daný kvantový systém reprezentovať a transformovať, na to aby sme boli schopní použiť kvantové princípy na výpočty, je nutné nejakým spôsobom výstup prečítať, teda uskutočniť meranie. A tu sa situácia odlišuje od klasických modelov, totiž kvantový stav sa meraním ovplyvní, a to tak vážne, že to znemožnuje jeho kopírovanie.

Postulát 3

Matematickým modelom merania stavu je množina podpriestorov $B_1, B_2, \ldots, B_k \subseteq H$ takých, že $B_1 \times B_2 \times \ldots \times B_k = H$ a $B_i \perp B_j$ pre $i \neq j$. Potom je možné vyjadriť stav $|\psi\rangle$ ako

$$|\psi\rangle = \sum_{i=1}^{k} \alpha_i |\psi B_i\rangle \ ,$$

kde $|\psi B_i\rangle$ je prvok podpriestoru B_i . Výsledok merania je jeden z podpriestorov B_i a to s pravdepodobnosťou $|\alpha_i|^2$. Stav $|\psi\rangle$ skolabuje do stavu získaného renormalizáciou $|\psi B_i\rangle$ [3].

Teda výsledkom merania je informácia, ktorý podpriestor bol vybraný, informácie mimo tohto podpriestoru su stratené. Ak by sme chceli merať našu superpozíciu čísel 1 a 5 a rozhodli sa použiť bázové stavy 0 až 7 ako podpriestory, dostali by sme v polovici prípadov

odpoveď 1 a v polovici 5. V dalšom budeme pracovať s touto, takzvanou kanonickou bázou. Práve kolaps stavov je dôvodom, prečo nie je možné kvantový stav kopírovať. To vedie na zaujímavú aplikáciu v oblasti kvantovej kryptografie. Ak by sa útočník pokúsil odpočúvať informácie, nedokázal by ich kopírovať a posielať v nezmenenej forme pôvodnému príjemcovi. To by strany, ktoré si napríklad potrebujú bezpečne vymeniť kľúč odhalili a nepoužili by ho. Kolaps taktiež ničí nádej na exponenciálnu paralelizáciu výpočtov, kedy by počítač dostal superpozíciu všetkých vstupov a podal by superpozíciu odpovedí ako výstup. Vídíme, že keby sme sa výstupný stav pokúsili merať, skolaboval by jednej z odpovedí a stratili by sme všetky ostatné. Avšak predsalen sa nejaká informácia vydolovať dá, dajú sa získavať odpovede globálnejšej povahy. Nedokážeme síce naraz získať hodnotu všetkých funkčných hodnôt určitej funkcie, ale dokážeme napríklad určiť jej periódu.

Kapitola 2

Teória čísel

2.1 Kryptosystém RSA

V tejto časti predstavíme v praxi veľmi rozšírený systém na ochranu informácii, RSA viz napr. [9]. Strany A a B potrebujú spolu bezpečne komunikovať. Dohodnú sa, že budú reprezentovať správy ako čísla. Strana A nájde dva rôzne prvočísla p , q a za N položí N = pq. Ďalej vypočíta hodnotu Eulerovej funkcie z N, $\phi(N)=(p-1)(q-1)$. Zvolí číslo e tak, aby bolo nesúdelné s $\phi(N)$ a $1<e<\phi(N)$. Nakoniec vypočíta d splňujúce $de\equiv 1 \, mod \, \phi(N)$. Na nachádzanie veľkých prvočísel sa používajú pravdepodobnostné algoritmy, ktoré vyberú kandidáta a overia, či sa jedná o prvočíslo napríklad pomocou

Rabin-Millerovho testu [8]. Číslo *d* sa zas ľahko nájde pomocou rozšíreného Euklidovho algoritmu, keďže máme nesúdelnosť *e* a $\phi(N)$. Strana A zverejní dvojicu (e,N), takzvaný verejný kľúč. To umožní strane B zašifrovať správu *t*, určenú pre A, ako $c = t^e \bmod N$. Ak teda A obdrží správu *c,* teda *t* v zašifrovanej podobe, stačí jej na dešifrovanie použiť svoj súkromný kľúč *d ,* ktorý nik iný nepozná. Vypočíta $t = c^d \bmod N$. To, že v skutočnosti dostane pôvodnú správu nahliadneme z toho, že $c^d = t^{de} = t^{1+S(P-1)(Q-1)} = t \bmod p$ a $c^d = t^{de} = t^{1+S(P-1)(Q-1)} = t \bmod q$ pričom využívame malú Fermatovu vetu a vidíme že kongurencie platia, aj keď *p* delí *t*. Máme $t^{de} - t$ deliteľné *q* aj *p,* teda aj *pq*. Dostávame $t^{de} = t \bmod N$. Bezpečnosť RSA je postavená na tom, že ak by chcela tretia strana dekódovať správu určenú pre A, musela by poznať *d,* na výpočet ktorého zas $\phi(N)$ a túto hodnotu by bola schopná zistiť len zo znalosti *p* a *q,* teda faktorov N. V súčastnosti faktorizácia na klasických počítačoch predstavuje pre veľké N neprekonateľný problém. Pozrime sa teraz na to, ako sa dá previesť probém rozkladu zloženého nepárneho čísla N na úlohu nájdenia rádu prvku v $\mathbb{Z}^*_N$ teda v grupe invertibilných prvkov s násobením modulo N. Rádom prvku $x \in \mathbb{Z}^*_N$ sa myslí najmenšie *r* také, že $x^r = 1 \bmod N$.

2.2 Rozklad cez rád

Predpokladajme, že máme k dispozícii procedúru ktorá nájde rád *r* prvku *x* v grupe $\mathbb{Z}^*_N$. Prepíšeme $x^r = 1 \bmod N$ na $(x^{r/2} - 1)(x^{r/2} + 1) = 0 \bmod N$ a ukážeme, že pre párne *r* a $x^{r/2} \neq -1 \bmod N$ je $NSD(x^{r/2} - 1, N)$ netriviálnym faktorom N. Označme $(x^{r/2} - 1)$ ako *u* a $(x^{r/2} + 1)$ ako *v.* $N \mid uv$ takže $Nk = uv$ pre nejaké *k.* Predpokladajme pre spor, že $NSD(x^{r/2} - 1, N) = 1$. Potom $mu + nN = 1$ pre nejaké *m, n* .

Vynásobením poslednej rovnosti *v* dostávame $mNk+nNv=v$ a teda $N|v$. To by implikovalo existenciu *h* takého, že $Nh-1=x^{r/2}$ a teda spor s predpokladom $x^{r/2}\neq -1 \, mod \, N$. Zostáva teda zistiť, ako často uvedený postup nefunguje, teda s akou pravdepodobnosťou dostaneme nepárne *r* alebo $x^{r/2}=-1 \, mod \, N$. Označíme rozklad čísla $N=\prod_{i=1}^{k} p_i^{a_i}$ a r_i rád *x* modulo $p_i^{a_i}$. Potom *r* je najmenší spoločný násobok všetkých r_i . Najväčšie d_i také že $2^{d_i}|r_i$ nazvime 2-valuáciou r_i . Ak sa zhodujú 2-valuácie r_i , dostávame sa do situácie, ktorá nevedie k cieľu. Skutočne, ak sú $d_i=0$ je *r* nepárne. V prípade $d_i\geqslant 1$ je $x^{r/2}=-1 \, mod \, N$ pretože $x^{r/2}=-1 \, mod \, p_i^{a_i}$ pre všetky *i*. Podľa Čínskej vety o zbytkoch je náhodný výber *x* modulo N to isté, ako náhodný výber x_i modulo $p_i^{a_i}$ pre všetky *i*. Grupa j $\mathbb{Z}^*_{p_i^{a_i}}$ je cyklická, preto máme najviac polovičnú šancu vybrať x_i ktorého rád má nejakú konkrétnu 2-valuáciu d_i . Teda ak vyberieme pre i =1 , pre i =2 narazíme na x_2 s $d_2=d_1$ s pravdepodobnosťou najviac $1/2$, a tak ďalej a teda vidíme že sa všety d_i zhodnú s pravdepodobnosťou najviac $1/2^{k-1}$. Pre prípad k=1, kedy je nepárne N mocninou prvočísla, už existujú efektívne faktorizačné algoritmy.

Kapitola 3

Kvantové výpočty

3.1 Budovanie kvantových brán

V tejto kapitole zostrojíme základné stavebné jednotky kvantového počítača, kvantové brány. Matematicky je kvantová brána unitárna transformácia, ktorá pôsobí na jeden alebo viac qubitov. Samozrejme výsledok môže slúžiť ako vstup pre ďalšiu kvantovú bránu. Takto naviazané brány tvoria kvantové obvody a umožnujú uskutočniť beh kvantového algoritmu na ktorý sú určené. Začneme najednoduchšou, Hadamardovou bránou H. Tá pôsobí na jeden qubit a jej účinok na jednotlivé bázové stavy je

$$H|0\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right) \qquad H|1\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right) \ .$$

V tvare unitárnej matice vyzerá Hdamardova brána ako

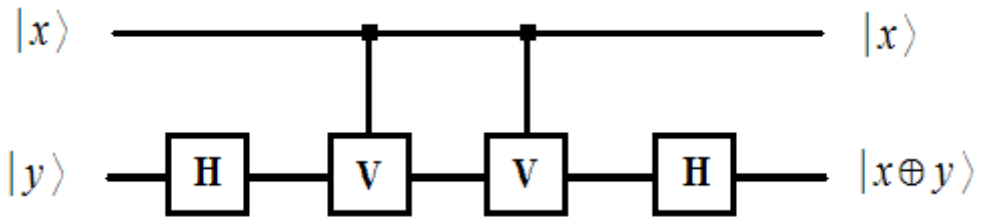
$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

takže $|x\rangle\rightarrow 1/\sqrt{2}\left((-1)^x|x\rangle+|1-x\rangle\right)$ pre x=0,1. Vidíme, že H umožnuje uviesť qubit v základnom bázovom stave do superpozície stavov. Ďalšou užitočnou bránou bude c-V brána, pôsobiaca na dvoch

qubitoch a to tak, že bázu transoformuje ako $|0\rangle|y\rangle \rightarrow |0\rangle|y\rangle$ $|1\rangle|y\rangle \rightarrow |1\rangle(V|y\rangle)$, teda v prípade, že prvý (kontrolný) qubit je 1 aplikuje na druhý unitárnu transformáciu

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} .$$

Skúsme skombinovať prvé dve brány podla nasledujúcej schémy.



Horizontálne čiary predstavujú vývoj stavov jednotlivých qubitov počas behu výpočtu z ľava do prava, štvorce zodpovedajú unitárnym transformáciám a vertikálne spoje graficky vyjadrujú že brána V je dvojqubitová. Dostávame bránu c-NOT. Pozrime sa, ako pôsobí na jednotlivé bázové stavy.

$$|0\rangle|0\rangle \rightarrow |0\rangle\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \rightarrow |0\rangle\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \rightarrow |0\rangle\left(\frac{1}{2}|0\rangle+\frac{1}{2}|0\rangle\right)=|0\rangle|0\rangle$$

$$|0\rangle|1\rangle \rightarrow |0\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \rightarrow |0\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \rightarrow |0\rangle\left(\frac{1}{2}|1\rangle+\frac{1}{2}|1\rangle\right)=|0\rangle|1\rangle$$

$$|1\rangle|0\rangle \rightarrow |1\rangle\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle) \rightarrow |1\rangle\frac{1}{\sqrt{2}}(|0\rangle+i^2|1\rangle) \rightarrow |1\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \rightarrow |1\rangle|1\rangle$$

$$|1\rangle|1\rangle \rightarrow |1\rangle\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle) \rightarrow |1\rangle\frac{1}{\sqrt{2}}(|0\rangle-i^2|1\rangle) \rightarrow |1\rangle\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \rightarrow |1\rangle|0\rangle$$

V prípade, že je horný qubit v stave 0, dolný zostane nezmenený. Ak je však v stave 1, zneguje hodnotu dolného. Preto názov controlled NOT. Mohli sme c-NOT bránu vyjadriť rovno ako c-U kde transformácia

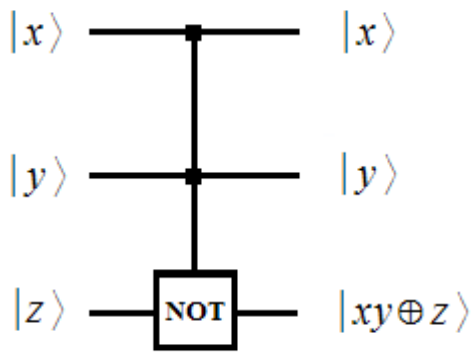
$$\mathrm{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

prehadzuje dolný qubit. Podobne môžme pripraviť tretiu bránu, c-PS (ϕ) z anglického controlled phase shift, transformácia dolného qubitu bude v maticovom zápise vyzerať nasledovne

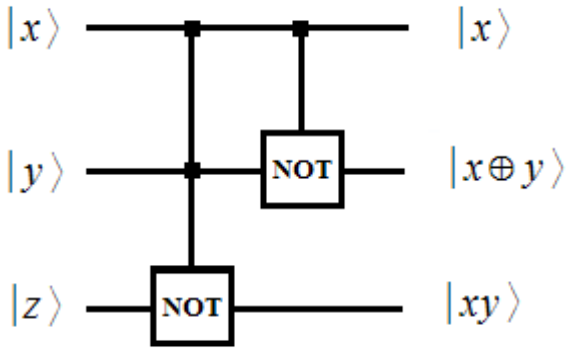
$$\mathrm{U}\ (\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Brána c-PS (ϕ) na bázový stav $|x\rangle|y\rangle$ pôsobí ako $e^{ixy\phi}|x\rangle|y\rangle$, dochádza k posunu fázy o ϕ, v prípade že x = y = 1.

Konštrukcia c-NOT pomocou Hadamardových a c-V brán pekne ilustruje, ako sa pomocou málo jednoduchých stavebných blokov dajú vyrobiť zložitejšie, čo je žiadané, keď sa fyzicky navrhuje kvantový obvod. Odpadá totiž nutnosť hľadať fyzikálnu reprezentáciu samostatne pre každú použitú bránu. Pozrime sa na to, ako sa dá na kvatovom počítači vyhodnocovať funkcia AND a sčítať modulo 2. Budeme na to potrebovať controlled-controlled-NOT bránu. Tá zneguje tretí qubit ak su prvé dva v stave 1. Ak ju použijeme na tri qubity v stavoch $|x\rangle|y\rangle|z\rangle$ x,y,z = 0,1 dostaneme



čo zodpovedá funkcii $|x\rangle|y\rangle|z\rangle \rightarrow |x\rangle|y\rangle|((x \wedge y)\oplus z)\rangle$. Nastavením posledného qubitu na 0 dostávame AND, v opačnom prípade negáciu AND. Na sčítanie modulo 2 použijeme



teda jeden c-c-NOT a jeden c-NOT. Aj bránu c-c-NOT je možné skonštruovať pomocou Hadamardových a c-V brán [5]. Postupne takto ide vybudovať kvantové sčítanie, z neho násobenie a mocnenie modulo N. Práve modulárne mocnenie využijeme počas algoritmu na faktrorizáciu. Poznamenajme, že všetky brány musia byť unitárne transformácie, teda invertibilné. Na klasických počítačoch sčítanie invertibilné nieje, avšak na kvantových áno. Pripravme si teraz bránu, ktorá je jadrom kvantovej faktorizácie. Označíme ju QFT, Qantum Fourier Transform. Ukážeme, že je možné vybudovať ju použitím H a

c-PS (ϕ) brán. Jedná sa o viacqubitovú bránu, ktorá transformuje bázový stav $|a\rangle$ l qubitového registra, kde a je vyjadrené v dvojkovej sústave ako $a=\sum_{i=0}^{l-1} a_i 2^i$, nasledovne :

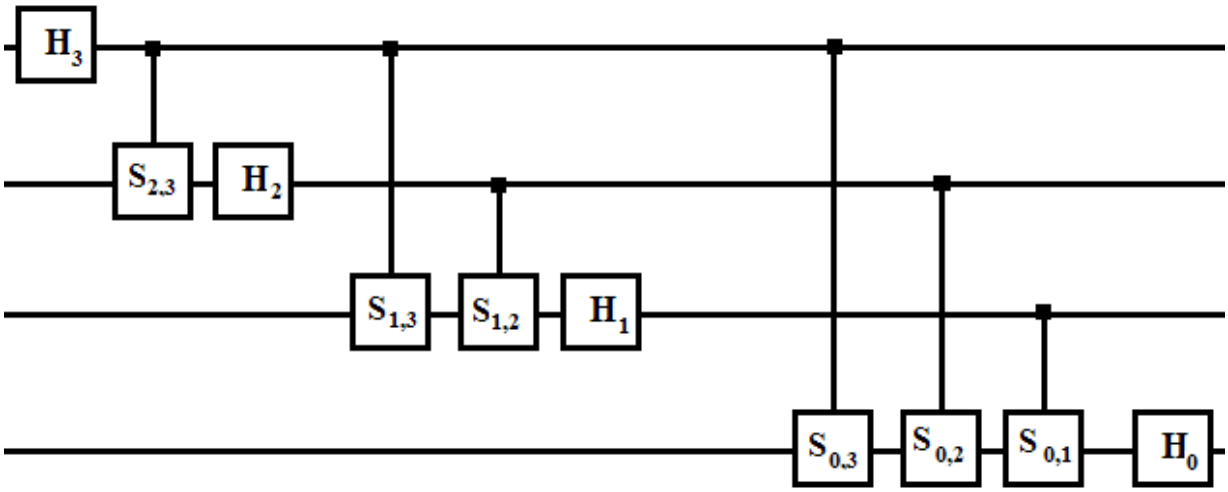
$$QFT|a\rangle=\frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}\exp\left(\frac{2\pi i a c}{q}\right)|c\rangle \quad \text{kde} \quad q=2^l$$

a $|c\rangle$ prebieha všetkých q bázových stavov l qubitového registra. Hadamardovú bránu pôsobiacu na j-ty qubit označme H_j a nech $S_{j,k}$ symbolizuje $c-PS\left(\pi/2^{k-j}\right)$ aplikovanú na j-ty a k-ty qubit, j< k.

Vytvoríme z nich naseldovnú sieť :

$$H_{l-1}S_{l-2,l-1}H_{l-2}S_{l-3,l-1}S_{l-3,l-2}H_{l-3}\ldots H_1 S_{0,l-1}S_{0,l-2}\ldots S_{0,2}S_{0,1}H_0$$

Napríklad na štyroch qubitoch vyzerá sieť takto,



čo zapíšeme ako $H_3S_{2,3}H_2S_{1,3}S_{1,2}H_1S_{0,3}S_{0,2}S_{0,1}H_0$. Pozrime sa na navrhnutú l qubitovú sieť detailnejšie, sledujme akú hodnotu vnesie pred bázový stav $|c\rangle$, ak ju aplikujeme na $|a\rangle$. V nasledujúcom ukážeme, že dostaneme QFT, len bude treba čítať binárne vyjadrenie c v opačnom poradí. Výsledná amplitúda pri nejakom bázovom stave

$|b\rangle$ je ovplyvnená len bránami H_j , brány $S_{j,k}$ menia iba fázu. Každá H_j prispieva k výslednej amplitúde pri $|b\rangle$ faktorom $1/\sqrt{2}$, a tieto príspevky sa vynásobia na $1/\sqrt{2^l}$, kedže používame celkovo l H_j brán. Teda pri každom $|b\rangle$ je v sume komplexné číslo velkosti $1/\sqrt{q}$. Po vyňatí $1/\sqrt{q}$ pred sumu vidno, že stačí overiť, že súhlasia fázy pri jednotlyvých bázových stavoch. Majme $|b\rangle$ dvojkovo vyjadrené ako $|b_{l-1}b_{l-2}...b_0\rangle$ a sledujme, čo prispieva k jeho konečnej fáze. Postupne transformujeme stav $|a_{l-1}a_{l-2}...a_0\rangle=|a_{l-1}\rangle|a_{l-2}\rangle...|a_0\rangle$ a všimneme si, že a_j prechádza na b_j jedine pôsobením brány H_j ktorá mení fázu len v prípade $a_j=b_j=1$ a to tak, že k nej pridá π . Využívame $-1=e^{i\pi}$ a mechanizmus pôsobenia Hadamardovej brány $|a_i\rangle\rightarrow 1/\sqrt{2}\left((-1)^{a_i}|a_i\rangle+|1-a_i\rangle\right)$ $a_i=0,1$ Taktiež brány $S_{j,k}$ pridávajú $\pi/2^{k-j}$ ak sú $a_j=b_j=1$, inak neprispejú nič. Celkový príspevok do fázy $|b\rangle$ možme vyjadriť ako

$$\sum_{0\leq j<l}\pi a_j b_j+\sum_{0\leq j<k<l}\frac{\pi}{2^{k-j}}a_j b_k$$

čo prepíšeme na

$$\sum_{0\leq j\leq k<l}\frac{\pi}{2^{k-j}}a_j b_k$$

a prehodením poradia vyjadrenia *b* a označením ho ako *c,* máme

$$\sum_{0\leq j\leq k<l}\frac{\pi}{2^{k-j}}a_j c_{l-1-k}$$

Substitúciou $r = l - k - 1$ dostávame

$$\sum_{0 \leqslant j+r<l} 2\pi \frac{2^j 2^r}{2^l} a_j c_r$$

Ak by sme sčítali aj cez $j+r \geqslant l$ pridávali by sme celočíselné násobky 2π a teda by to nemalo na fázu vplyv. Môžeme teda sčítať cez všetky j , $r < l$.

$$\sum_{j,r=0}^{l-1} 2\pi \frac{2^j 2^r}{2^l} a_j c_r = \frac{2\pi}{2^l} \sum_{j=0}^{l-1} 2^j a_j \sum_{r=0}^{l-1} 2^r c_r$$

kedže $q = 2^l$ dostávame $(2\pi i a c)/q$. Takže, po aplikovaní našej siete dostávame

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \exp\left(\frac{2\pi i a c}{q}\right) |b\rangle$$

kde dvojkové vyjarenie c je vyjadrenie $b,$ ale čítané v opačnom poradí. Teda sieť produkuje QFT, jedine treba čítať odzadu dvojkový zápis obdržaných bázových vektorov, čo z hladiska implementácie nepredstavuje problém [1]. Ukázali sme taktiež, že síce $q = 2^l$ rastie exponenciálne , na QFT postačuje $l(l-1)/2$ brán.

Kapitola 4

Kvantové algoritmy

4.1 Algoritmus Deutsch-Jozsa

Máme k dispozícii slušný repertoár brán, je načase demonštrovať silu kvantových počítačov na konkrétnom algoritme [8]. Budeme pracovať s funciou $f:\{0,1\}^n \to \{0,1\}$, o ktorej vieme, že je buď konštantná alebo vyvážená (na polovici x dáva 0 na polovici 1). Ďalej máme prístup k jej kvantovej implementácii v podobe orákula, ktoré vyhodnocuje $|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$. Chceme rozhodnúť, či je funkcia konštantná alebo vyvážená, s čo najmenším počtom dotazov. Vidíme, že klasickým spôsobom dostaneme správnu odpoveď v najlepšom prípade po dvoch dotazoch, v najhoršom ich však potrebujeme $2^{n-1}+1$. Algoritmus, ktorý predstavíme, odpovie vždy správne po jednom dotaze. Pripravíme si n+1 qubitový register do stavu $|0\rangle^n|1\rangle$. Aplikujeme na každý qubit Hadamardovu transformáciu. Dostaneme stav

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|0\rangle-|1\rangle\right)$$

použijeme na neho orákulum . Obdržíme

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|f(x)\rangle-|1\oplus f(x)\rangle\right)$$

čo, prebratím možností hodnôt $f(x)$ prepíšeme na

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\left(|0\rangle-|1\rangle\right)$$

Aplikujeme zas H na každý qubit v predošlom výraze, okrem posledného, ktorý odteraz ignorujeme. Ako H transformuje $|x\rangle$?

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \odot y} |y\rangle$$

kde $x \odot y = x_{n-1} y_{n-1} + x_{n-2} y_{n-2} + \ldots + x_0 y_0$. To nahliadneme z toho, že $|y\rangle$ vzniká z výsledkov aplikácie H na jednotlivé qubity $|x\rangle$ nasledovne

$$|x\rangle = |x_{n-1}\rangle \ldots |x_0\rangle \rightarrow$$

$$\frac{1}{\sqrt{2}} \left((-1)^{x_{n-1}} |x_{n-1}\rangle + |1 - x_{n-1}\rangle \right) \ldots \frac{1}{\sqrt{2}} \left((-1)^{x_0} |x_0\rangle + |1 - x_0\rangle \right) .$$

Teda po *n* Hadamamardových bránach máme

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \otimes y} |y\rangle \quad ,$$

prepísateľné na

$$\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \left((-1)^{f(x)} (-1)^{x \otimes y} \right) |y\rangle \ .$$

Nakoniec skutočníme meranie. Vidíme, že pravdepodobnosť zmerania tohto stavu ako $|0\rangle^n$ tj.

$$\left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2$$

je 1, ak je funkcia konštantná a 0, ak je vyvážená. Včom spočíva toto exponenciálne zlepšenie oproti klasickému prístupu? Naraz sme orákulu poskytli všetky vstupy v superpozícii a aj keď sme nedostali

priamo všetky hodnoty funcie, šikovným manipulovaním sme boli schopní zistiť globálnu vlastnosť, takú na ktorej sa všetky hodnoty podielali.

4.2 Kvantové hľadanie rádu

Predošlý algoritmus nemá príliš velké praktické využitie, snáď s výnimkou robenia dojmu na sponzorov, ten, ktorý predstavíme teraz je však natoľko zásadný, že snaha o jeho fyzickú realizáciu významne poháňa výskum v oblasti kvantových počítačov. Ide o centrálnu čast Shorovho algoritmu na faktorizovanie [1], kvantové hľadanie rádu prvku v $\mathbb{Z}^*_N$. Ukážeme, že po sérií transformácii budeme s veľkou pravdepodobnosťou merať práve také stavy, ktoré nám ho umožnia nájsť. Majme teda *x* ktorého rád *r* chceme zistiť. Najdeme $q = 2^l$ pre nejaké l také, že $N^2 < q < 2\mathrm{N}^2$. Pripravíme si dva registre dĺžky *l* do stavu $|0\rangle^l |0\rangle^l$. Pomocou brán H použitých na prvý register si dostaneme stav

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |0\rangle \ .$$

Aplikujeme kvantovú implementáciu modulárneho mocnenia $|x\rangle|0\rangle \rightarrow |x\rangle|x^a \ mod \ N\rangle$, jeho výstavbu sme už naznačili v tretej kapitole. Ešte sa však k nemu vrátime, vplýva totiž na celkovú zložitosť. Do druhého registra sa dostanú hodnoty po mocnení.

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a \ mod \ N\rangle$$

Ďalej, na prvý register použijeme QFT. Zostaneme v stave

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp\left(\frac{2\pi i a c}{q}\right) |c\rangle |x^a \ mod \ N\rangle \ .$$

Uskutočníme meranie na všetkých qubitoch. Aká je pravdepodobnosť, že výsledkom bude nejaký konkrétny stav $|c\rangle|x^k \bmod N\rangle$, $0 \leqslant k < r$? Dostaneme ju ako

$$\left| \frac{1}{q} \sum_{a:\, x^a = x^k \bmod N} \exp\left(\frac{2\pi i a c}{q} \right) \right|^2 ,$$

ale taktiež môžme sčítať cez a: a mod $r = k$, vzhľadom na to že r je rád x. Položme $a = br + k$ a prepíšme podľa toho sumu vo vyjadrení pravdepodobnosti na

$$\left| \frac{1}{q} \sum_{b=0}^{[(q-k-1)/r]} \exp\left(\frac{2\pi i (br+k) c}{q} \right) \right|^2 ,$$

kde [ ] symbolizuje dolnú celú časť. Člen $\exp(2\pi i k c/q)$ vyberieme pred sumu a kedže ma veľkosť 1, nemusíme ho uvažovať. Pravdepodobnosť sa taktiež nezmení, ak cr nahradíme číslom kongurentným s cr mod q, ktoré označíme $\{cr\}_q$ s tým, že $-q/2 < \{cr\}_q \leqslant q/2$. Ukážeme, že ak je $\{cr\}_q$ malé, výsledná pravdepodobnosť je veľká, čo nám následne umožní nájsť r. Sumu v takto prepísanej pravdepodobnosti

$$\left| \frac{1}{q} \sum_{b=0}^{[(q-k-1)/r]} \exp\left(\frac{2\pi i b \{cr\}_q}{q} \right) \right|^2$$

aproximujeme integrálom nasledovne

$$\frac{1}{q} \int_0^{[(q-k-1)/r]} \exp\left(\frac{2\pi i b \{cr\}_q}{q} \right) db \quad +$$

$$O\left(\frac{[(q-k-1)/r]}{q} \left(\exp\left(\frac{2\pi i b \{cr\}_q}{q} \right) - 1 \right) \right)$$

Pre $\left|\{cr\}_q\right| \leqslant r/2$ je chybový člen $O(1/q)$. Poznamenajme, že podmienka $\left|\{cr\}_q\right| \leqslant r/2$ nezávisí na *k* , čoho využijeme neskôr. Po substitúcii *u= rb/q* dostávame

$$\frac{1}{r} \int_0^{[(q-k-1)/r]\frac{r}{q}} \exp\left(\frac{2\pi i u\{cr\}_q}{r}\right) du \ .$$

Kedže *k < r,*

$$\frac{1}{r} \int_0^1 \exp\left(\frac{2\pi i u\{cr\}_q}{r}\right) du$$

sa líši len o $O(1/q)$ od pôvodného integrálu. Jeho absolútna hodnota je najmenšia pre $\left|\{cr\}_q\right| = r/2$ a vychádza $2/(\pi r)$. Konečne, umocnením na druhú dostávame dolný odhad pre pravdepodobnosť pozorovania stavu $|c\rangle|x^k \bmod N\rangle$, za predpokladu $\left|\{cr\}_q\right| \leqslant r/2$, teda hodnotu $4/(\pi^2 r^2) + O(1/q)$, čo je aspoň $1/(3r^2)$ pre dosť velké N, pri ktorom sú už chyby v odhadoch dostatočne malé. Podmienku $\left|\{cr\}_q\right| \leqslant r/2$ je možné vyjadriť aj ako existenciu *d* takého, že $-r/2 \leqslant rc - dq \leqslant r/2$. Po vydelení *rq* ekvivalentne $\left|c/q - d/r\right| \leqslant 1/(2q)$. Odmerali sme *c*, poznáme *q*, skúsme zaokrúhliť zlomok c/q na najbližší zlomok d/r , ktorý ma menovateľ menší ako *n* a spĺňa poslednú podmienku $\left|c/q - d/r\right| \leqslant 1/(2q)$. Takýto zlomok existuje maximálne jeden. Ak by existoval, a mal naviac *d* a *r* nesúdelné, dostali by sme z neho *r.* Koľko stavov $|c\rangle|x^k \bmod N\rangle$ vedie pri použití tohoto postupu úspešne k cieľu? Počet zlomkov d/r s nesúdelným čitateľom a menovateľom udáva Eurlerova funkica, je ich $\phi(r)$. Každý takýto zlomok je blízko nejakému c/q s $\left|c/q - d/r\right| \leqslant 1/(2q)$. Kedže *x* má rád *r,* x^k nadobúda *r* rôznych hodnôt a dostávame $r\phi(r)$ stavov

$|c\rangle|x^k \bmod N\rangle$, ktoré nám umožnia nájsť *r*. Každý uvidíme s pravdepodobnosťou aspoň $1/(3r^2)$ teda úspech nastáva minimálne s pravdepodobnosťou $\phi(r)/(3\mathrm{r})$. Z odhadu $\phi(r)/r > \delta_1/(\log\log r)$ vidno že nájdeme *r* aspoň $\delta_2/(\log\log r)$ času pre nejakú konštantu δ_2 . Vysokú pravdepodobnosť úspechu teda dosiahneme, ak budeme opakovať postup $O(loglog(r))$ krát. Pozrime sa na vylepšenia, realizované klasicky, ktoré nachádzajú dalších kandidátov na rád . Ak by sme dostali po zaokrúhlení *d* a *r,* ktoré majú spoločný deliteľ, je pravepodobné že bude malý. Preto je výhodné uvažovať za kandidátov aj malé násobky *r′,* kde *d′* a *r′* už predstavujú zlomok v základnom tvare. Tak isto je vhodné uvažovať najmenší spoločný násobok dvoch kandidátov. Ukazuje sa, že tieto techniky umožnujú znížiť počet počet opakovaní postupu z $O(loglog(r))$ na $O(1)$ a to aj pre najťažšie N. Uvedené zaokrúhlenie sa dá urobiť v polynomiálnom čase pomocou rozvinutia c/q do reťazového zlomku pomocou ktorého sa nájdu všetky dobré aproximácie. Odhady a vyplešenia detailnejšie v [1].

4.2 Shorov algoritmus

Máme dané nepárne zložené číslo N ktorého rozklad hľadáme. Shorov faktorizačný algoritmus vyzerá nasledovne:

1.Vyber náhodne $x < N$.

2. Vypočítaj $NSD(x, N)$, ak sa nerovná jedna, našli sme netriviálny faktor. Inak pokračuj krokom 3.

3. Nájdi rád *r* prvku *x* modulo N. Ak je *r* nepárne, alebo $x^{r/2} = -1 \bmod N$ vráť sa na 1, inak pokračuj krokom 4.

4. Vypočítaj $NSD(x^{r/2} - 1, N)$, našli sme netriviálny faktor N.

Po konečnom počte opakovaní dostávame celý rozklad čísla N a v prípade hľadania rozkladu N = *pq* , napríklad pre RSA, stačí uvedený postup sledovať raz a druhé prvočíslo dopočítať klasicky. Pozrime sa bližšie na zložitosť jednotlivých krokov. Zaujíma nás časová náročnosť závislá od dĺžky vstupu, teda počtu bitov *l* čísla N. Zložitosť kvantovej časti, teda kroku 3, udáva efektivita modulárneho mocnenia. Ukázali sme že QFT sa dá uskutočniť na $O(l^2)$ bránach, ktoré predstavujú jednotku výpočetnej zložitosti. Najlepší klasický postup pre modulárne mocnenie $x^r \bmod N$ prebieha tak, že sa opakovaným mocnením na druhú pripraví $x^{2^i} \bmod N$ pre $i \leqslant \log_2(r)$ a potom vynásobí podmnožinu týchto mocnín podľa toho, kde sa v dvojkovom zápise *r* objaví 1. Vyžaduje teda $O(l)$ násobení a mocnení na druhú. Na násobenie dvoch *l* bitových čísel spotrebujeme $O(l^2)$ operácií pri použití školského násobenia, celkovo teda $O(l^3)$ pre modulárne mocnenie. Pre kvantovú verziu modulárneho mocnenia môžme použiť ten istý postup avšak musíme pamätať na to, že všetky operácie musia byť invertibilné, čo při naivnom prístupe znamená uchovávať medzivýsldky, teda nárast nárokov na miesto. A kedže Euklidov algoritmus potrebuje $O(l^2)$ operácií, vidíme že sme stále v medziach kubickej zložitosti. Existuje mnoho vylepšení používajúcich rýchlejšie algoritmy na násobenie alebo redukujúcich nárast nárokov na miesto, ktoré vzniknú zaručením, aby bolo násobenie invertibilné. Vhodnosť ich použitia závisí od veľkosti faktorizovaného čísla, pokročilé algoritmy sú prakticky rýchlejšie až pre vačšie *l.* V každom prípade je polynomiálny algoritmus na faktorizáciu senzáciou, pretože najlepší klasický má stále exponeniálnu zložitosť ,

$$O\left(\exp\left(\left(\frac{64}{9}l\right)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right)\right)$$

[6]. Dôsledky takto rýchleho faktorizovania pre informačnú bezpečnosť sú obrovské, ak by reálne existoval kvantový počítač s

dostatočným počtom qubitov, umožnoval by prelamovať šifry, ako napríklad RSA, momentálne považované za bezpečné a masovo rozšírené v praxi.

Kapitola 5

Kvantové počítače v praxi

5.1 Fyzikálna realizácia, budúcnosť

Ak chceme kvantové výpočty úspešne previesť do praxe, narazíme na radu problémov. Ako reprezentovať qubit? Ako konštruovať brány tak, aby skutočne zodpovedali žiadaným unitárnym transformáciám? Na uchovanie kvantovej informácie sa ponúkajú mikroskopické systémy ktoré vykazujú kvantové správanie, napríklad polarizované fotóny. Otázka nájdenia vhodného hardvéru ešte stále nieje uzavretá, avšak všetky návrhy zápasia s rovnakým nepriateľom. Tým je takzvaná dekoherencia, teda interakcia počítača a okolitého prostredia počas priebehu výpočtu, kedy vonkajší svet uskutočnuje nechcené predčasné merania, kolaps stavov a stratu informácie. Existujú postupy ktoré znižujú tieto vplyvy, robia kvantový systém odolnejší. Rieši sa problém previesť kvantové správanie na mikroskopickej úrovni do väčších rozmerov, ktoré sú inžiniersky ľahšie realizovateľné. V oblasti kvantových výpočtov vidno veľký pokrok, podarilo sa úspešne demonštrovať Shorov algoritmus na sedem qubitovom počítači, faktorizovaním čísla 15. V roku 2007 bol predstavený firmou D-WAVE [11] prvý komerčne použiteľný počítač so 16 qubitmi, v roku 2008 ho tvorcovia zlepšili na 28 qubitov. Kvantový procesor,

učený na riešenie rodiny problémov do ktorej patrí napríklad porovnávanie fotiek, je chladený na teplotu 10 mK, aby sa dekoherencia udržala na prijateľnej úrovni. D-WAVE hovorí o dostupnosti 512 a 1024 qubitového počítača v najbližších rokoch, čo už prinesie znateľný nárast výkonu oproti klasickým počítačom pri riešení niektorých problémov. Aké sú teda vízie vzdialenejšej budúcnosti? Určite sa nepredpokladá, že by kvantové počítače plne nahradili súčasné, stále je mnoho úloh praktickejšie počítať klasicky, kvantový prístup sa hodí len na podskupinu úloh. Pravdepodobne budú spočiatku dostupné pre komerčné využitie v špecializovaných strediskách, na ktoré sa budú pripájať klasické počítače v tej fáze behu výpočtu, ktorá je klasicky príliš náročná a vyžaduje kvantový prístup. Kvantová mechanika popisuje správanie sveta, ktoré je ľudskej intuícii vzdialené, objavujú sa podivné interpretácie fenoménu superpozície ako napríklad známa Schrödingerova mačka. Tá je v uzavretej krabici zároveň mŕtva a živá, kedže vypustenie jedu závisí na mikroskopickom kvantovom jave, ktorý kvantová mechanika popisuje ako superpozíciu dvoch možných výsledkov a udáva len pravdepodobnosti ich zmerania. Až otvorenie krabice, teda zmeranie systému donúti systém skolabovať do jedného zo stavov. Možno sa však ukáže, že kvantové javy nie sú ľudskej mysli až tak vzdialené, objavujú sa indície, že ľudský mozog využíva na vyššie kognitívne funkcie kvantové princípy a teda že každý z nás nosí v hlave svoj vlastný kvantový počítač.

Literatúra

[1] Peter W. Shor : Revised version of *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,* Proceedings of the 35th Annual Symposium on Foundations of Computer science, Santa Fe, NM, Nov. 20-22, 1994, IEEE Comptuer Society Press, pp.124-134, arXiv:quant-ph/9508027v2

[2] Mathew Johnson : *Quantum Mechanics In Quantum Computing, B.S* Undergraduate Mathematics Exchange, Vol. 1, No.1 Fall 2003 p. 29-30

[3] André Berthiaume : *Quantum Computation,* Complexity Theory Retrospective II, Springer-Verlag, 1996 p. 8

[4] R. Feynmann : *Simulating physics with computers,* Int. J. Theor. Phys. 21, 467 ,1982.

[5] http://www.quantiki.org/wiki/index.php/Basic_

concepts_in_quantum_computation

[6] http://en.wikipedia.org/wiki/Integer_factorization

[7] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca (1998). *Quantum algorithms revisited*, Proceedings of the Royal Society of London A 454: 339–354.

[8] René Schoof, *Four primality testing algorithms*, to appear in: Surveys in algorithmic number theory, Cambridge University Press, Section 1

[9] http://www.di-mgt.com.au/rsa_alg.html

[10] Rivest, R.; A. Shamir; L. Adleman *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,* Communications of the ACM 21 (2):1978 pp.120-126.

[11] http://www.dwavesys.com/